CITY OF CORAL GABLES
IDENTITY THEFT PREVENTION PROGRAM

I. Purpose

The City of Coral Gables establishes this identity theft prevention program pursuant to the Federal Trade Commission's red flag rule, which implements Section 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

Under the red flag rule, the identity theft prevention program must be tailored to the entity's size, complexity, and nature of its operations. The basic elements of the identity theft prevention program are as follows:

1. Identify relevant red flags for covered accounts and incorporate them into the identity theft prevention program;

2. Detect red flags that have been incorporated into the identity theft prevention program;

3. Respond appropriate to any red flags that are detected to prevent and mitigate identity theft; and

4. To ensure the identity theft prevention program is updated periodically to reflect changes and risks to customers or to the safety and soundness of the City.

II. Definitions

The red flag rule defines "identity theft" as "fraud committed using the identifying information of another person; and a "red flag" as a "pattern, practice, or specific activity that indicates the possible existence of identity theft.

The red flag rule defines creditors to include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. According to the red flag rule, a municipal utility is a creditor subject to the red flag rule requirements. All the City's accounts that are individual utility service accounts held by customers of the utility whether residential, commercial or industrial are covered by the red flag rule. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors. The red flag rule also covers any other account that the City offers or maintains for which there is reasonably foreseeable risk to customers or to the safety and soundness of the City from identity theft, including financial, operations, compliance, reputation or litigation risks.

"Identifying information" is defined under the red flag rule as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's internet protocol address, or routing code.

III. Identification of red flags

In order to identify relevant red flags, the City considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with identity theft. The City identifies the following red flags and will train appropriate staff to recognize these red flags as they are encountered in the ordinary course of business:

A. Alerts, notifications or warnings from a consumer reporting agency

1. Report of fraud accompanying a credit report;

2. Notice or report from a credit agency of a credit freeze on a customer or applicant;

3. Notice or report from a credit agency of an active duty alert for an applicant;

4. Notice or report from a credit agency of an address discrepancy; and

5. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity. For example:

   a. An unusual increase in the volume of credit inquiries;
   b. Unusual increase in the number of established credit relationships;
   c. A material change in the use of credit, especially with respect to recently established credit relationship; or
   d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

B. Suspicious documents

1. Identification document or card that appears to be forged, altered or inauthentic;

2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;

3. Other document with information that is not consistent with information provided by the person opening a new covered account, by the customer presenting the identification, or with existing customer information on file with the City; and

4. Application for service that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. Suspicious personal identifying information

1. Identifying information presented that is inconsistent with other information the customer provides. For example, there is a lack of correlation between the social security number range and date of birth;

2. Identifying information presented that is inconsistent with external sources of information. For example:

a. The address does not match any address in the consumer report; or
b. The social security number has not been issued, or is listed on the Social Security Administration's Death Master File.

3. Identifying information presented is associated with known fraudulent activity. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or
b. The phone number on an application is the same as the number provided on a fraudulent application.

4. Identifying information presented that is commonly associated with fraudulent activity. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or
b. The phone number is invalid, or associated with a paper or answering service.

5. Social security number presented is the same as one given by another customer;

6. An address or telephone number presented is the same as that of another person;

7. A person fails to provide complete personal identifying information on an application when reminded to do so; and

8. A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious account activity or unusual use of account

1. Change of address for an account followed by a request to change the account holder's name;

2. Payments stop on an otherwise consistently up-to-date account;

3. Account used in a way that is not consistent with prior use. For example,

   a. Nonpayment where there is no history of late or missed payments;
   b. A material increase in the use of available credit;
   c. A material change in purchasing or spending patterns;
   d. A material change in electronic fund transfer patterns in connection with a deposit account; or
   e. A material change in telephone call patterns in connection with a cellular phone account.

4. Mail sent to the account holder is repeatedly returned as undeliverable;

5. Notice to the City that a customer is not receiving mail sent by the City;

6. Notice to the City that an account has unauthorized activity;

7. Breach in the City's computer system security; and

8. Unauthorized access to or use of customer account information.

E. Alerts from others

Notice to the City from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in identity theft.

IV. Preventing and mitigating identity theft

In the event City employees detect any identified red flags, such employees should contact the Director of Water & Sewers Department and/or the Finance Director. The Director of Water & Sewers Department and/or Finance Director will then decide which of the following steps should be taken:

1. Continue to monitor an account for evidence of identity theft;

2. Contact the customer;

3. Change any passwords or other security devices that permit access to accounts;

4. Not open a new account;

5. Close an existing account;

6. Reopen an account with a new number;

7. Notify law enforcement; or

8. Determine that no response is warranted under the particular circumstances.

V. Identity theft prevention program updates

This identity theft prevention program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the City's identity theft prevention program from identity theft. The City will consider the City's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the City maintains, and changes in the City's business arrangements with other entities. After considering these factors, the City will determine whether changes to the identity theft prevention program, including the listing of red flags, are warranted. If warranted, the City will update the identity theft prevention program.

VI. Identity theft prevention program administration

A. Oversight

The Director of Water & Sewers Department and/or Finance Director will be responsible for the identity theft prevention program's administration, for ensuring appropriate training of employees, for reviewing any reports regarding the detection of red flags and the steps for preventing and mitigating identity theft, for determining which steps of prevention and mitigation should be taken in particular circumstances, and for considering periodic changes to the identity theft prevention program.

B. Employee training and reports

City employees responsible for implementing the identity theft prevention program shall be trained either by or under the direction of the Director of Water & Sewers Department and/or Finance Director in the detection of red flags and the responsive steps to be taken when a red flag is detected. City employees should prepare a report at least annually for the Director of Water & Sewers Department and/or Finance Director, including an evaluation of the effectiveness of the identity theft prevention program with respect to opening accounts, existing covered accounts, service provider arrangements, significant incidents involving identity theft and responses, and recommendations for changes to the identity theft prevention program.

C. Service provider arrangements

In the event the City engages a service provider to perform an activity in connection with one or more accounts, the City will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft:

1. Require that service providers have such policies and procedures in place; and

2. Require that service providers review the City's identity theft prevention program and report any red flags to the Director of Water & Sewers Department and/or Finance Director.